**Senate Standing Committee on Economics**

ANSWERS TO QUESTIONS ON NOTICE

**Treasury Portfolio**

Budget Estimates

4 – 6 June 2013

**Question:** **BET 768**

**Topic:** **Protective Security Policy Framework**

**Written:** **17 June 2013**

**Senator BUSHBY asked:**

768. Provide an update for your department/agency, including what is your current compliance level, what are you doing to manage risk, what is being done to comply with the mandatory requirements and details of any department/agency specific policies and procedures.

**Answer:**

768. The Protective Security Policy Framework (PSPF) requires agencies to use risk management principles and policies appropriate to the agencies' functions and security threats in developing and maintaining their protective security measures.

The Australian Prudential Regulation Authority (APRA) has changed the way it categorises its information and it is putting in place the necessary infrastructure, policies and procedures to meet the increased level of security. APRA will continue its implementation of these heightened security measures as part of its investment in and renewal of its infrastructure over the next few years to ensure it is compliant with the PSPF and international standards.

APRA manages all its key risks strategically and systematically. Through its Enterprise Risk Management Framework, APRA identifies, assesses, treats, monitors and reports to the APRA Members on its key risks, including security-related risks.

A dedicated Security Group at senior management level has responsibility for the oversight of APRA's Enterprise Security Management, including the coordination of the infrastructure, changes to policies and procedures and managing emerging security risks and threats.

APRA has a number of policies and standards in place or under review that cover the following areas:

- overall enterprise security policy, strategy and framework;
- physical access and security;
- personnel security and security vetting;
- electronic access and cryptography;
- records and document management;
- information classification;
- vulnerability management; and
- recovery and business continuity.